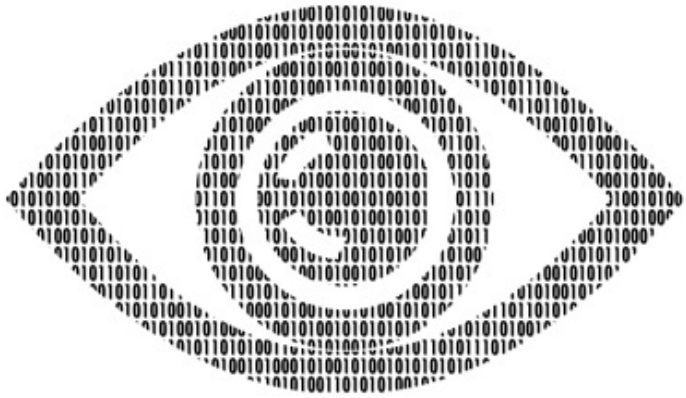
RETHINKING DIGITAL FREEDOM

Practices and technologies of intrusive surveillance in Turkey in relation to the EU



Utrecht University
MA. Thesis New Media and Digital Culture

Author: İlayda Şarlak
Date: 15-08-2016
First supervisor: dr. Ingrid Hoofd
Second supervisor: dr. Imar de Vries

To my grandmother, Sara.
My backbone, my inspiration.

-ily

PREFACE

I would like to take this opportunity to thank my supervisor Ingrid Hoofd for providing me constant support and supervision during my studies as well as Imar de Vries for helping me to gain new insights on this research.

I also wish to express my sincere gratitude to Jean Monnet Scholarship Program for making my master's education possible.

Many thanks go to Niall and Felicia for critically editing and reviewing this thesis.

Lastly, special thanks must go to my friends and my dearest family, Eva, Tayfun and Lara. They have been a pillar of support and have actively encouraged me throughout my studies.

TABLE OF CONTENTS

INTRODUCTION 1
CHAPTER 1: A CULTURAL APPROACH TO DISCOURSE 6
1.1. Language, Culture, Discourse 6
1.2. A Cultural View on Technologies 9
CHAPTER 2: PRIVACY AND FREEDOM IN THE DIGITAL AGE 11
2.1. Electronic Surveillance: When Technology Enhances State Power 11
2.2. Mapping the Discourse of Digital Freedom 15
CHAPTER 3: CIRCUIT OF SPYWARE 19
3.1. Turkey: A Look at the Actors and Technology 19
3.1.1. Representation 19
3.1.2. Moments of identity 22
3.1.3. Production 23
3.1.4. Consuming RCS 26
3.1.5. Regulation 29
3.2. EU as a 'Global Player' in the Digital Freedom 30
CONCLUSION 35
REFERENCES 39
PLAGIARISM STATEMENT 48

INTRODUCTION

In a recent hacking case, a woman received an e-mail whom she believed was from a trusted person who worked in a well-known academic institution. The e-mail referred to a subject that she was familiar with and contained a link to a website that had more information about the topic. However, she recognised that the e-mail address had a misspelling, and that the link was connected to a website in Turkey, where a malicious downloader file was about to be installed on her computer. She believed that she was targeted by forces in the Turkish government, associated with the powerful Gülen Movement that used to be an infiltrated part of the Turkish establishment. The American woman then found out that the downloader file had been linked to a spyware tool called the Remote Control System (RCS) purportedly sold by the Hacking Team exclusively to law enforcement and intelligence agencies around the world.

This particular story was taken from an article published in *Wired*, narrating the nature of challenges posed by Internet based technologies in the digital era (Zetter 2013). Undeniably, innovation in information technology has facilitated previously unanticipated forms of surveillance, namely storing, sharing and collecting the personal data of citizens. Over the past years, the Turkish government has systematically built up its capacity for intercepting electronically transmitted information (Shaw and Sentek 2016). Achieved by intrusive surveillance tools, Turkey successively developed the scope to hack into individual user devices and conduct targeted surveillance, which has undoubtedly become a matter of concern.

The reach of intrusive technologies is remarkably broad: listening into cell phone calls, using voice recognition to scan mobile networks, reading text messages and e-mails, tracking citizens' activity using GPS, and even changing e-mail contents while it is on its way to a recipient (Rodriguez 2016). In fact, according to Shaw and Sentek (2016) Turkey runs one of the most intrusive spying and surveillance infrastructures that can wiretap and conduct deep package inspection on Internet traffic.

The field of intrusive surveillance and breaches of privacy is a much-debated area. New technologies have brought extensive changes and challenges in almost every walk of our lives. Specifically, the growth of the online sphere has radically changed the landscape of freedom of expression in Turkey. In his book *Digital Freedom*, Batra (2008) addresses the notion of privacy and freedom as two sides of the same coin. In other words, privacy cannot be maintained without freedom and vice versa. Equally, violations on the right to privacy due to electronic surveillance prevents individuals from engaging in free speech. Therefore, each of them is a crucial prerequisite to the enjoyment of the other. Based on this rationale, the European Union (EU) has adopted digital freedom as a predominant strategy. Frequently referring to the issue in its statements, the EU constructed a discourse on the digital freedom, embracing it as an objective. This objective aims to foster rights in the digital sphere where the open and participatory nature of the Internet is guaranteed, and the right to privacy and freedom across the world is encouraged (Di Salvo 2013). Addressing the debate, recent studies (Caponetti 2016: Wagner and Bronowicka 2015) investigate the EU's strategy on the digital freedom and provide inspection on its objectives. Nonetheless, while in principle the EU desires to protect digital freedom, the compliance of candidate states remains questionable.

This is exemplified by a number of surveillance scandals that have rocked public confidence in the authorities' resort to such measures, in which Turkey has become part of this debate. Predominantly caused by the use of intrusive technologies, mass and targeted surveillance in Turkey highlights exactly where the right to freedom and privacy in the digital sphere is at risk (PEN International 2014). Therefore, being highly relevant to the EU's digital freedom discourse, the technologies of surveillance in Turkey has become a subject for examination, in relation to the EU. Whilst Europe is promoting digital freedom, it can be argued that Turkey is contributing to a surveillance market. Perhaps here we can explore the EU's dominant discourse of digital freedom by way of the intrusive tools Turkey both adopts and imports, to question whether surveillance is built into Turkey's infrastructure within the broader context of the EU. In the course of this, the following research question will be central: *To what extent do the practices and technologies of intrusive surveillance in Turkey corroborate or conflict with the discourse of digital freedom in relation to the EU?*

The theoretical framework of this study will provide a lens through which the qualitative research will be carried out. In order to capture the discursive aspects, I need to apply a theoretical framework which will allow the use of a 'meaning' based perspective on intrusive

technologies and provide a practical entry point to study the notion of digital freedom as a cultural value. On this basis, my aim is to posit the technologies of electronic surveillance, namely intrusive technologies, as the object of the research. Therefore, by using the *circuit of culture* framework, which is a theoretical perspective that brings together technology and culture (du Gay, Paul, Hall, Janes, Mackay and Negus 2002), I will attempt to show how meaning is produced at different sites, and circulated in a continuous process. The framework not only grounds this work, but also allows for an exploration of discursive production as a methodology. It can accommodate a macro-perspective of the wider circulation of a technology in Turkish society. As maintained by the framework, the world is perceived in a manner of cultural practice and as a cultural text that is fostered together within various moments (ibid). These moments enable technology to be represented as a dialectic where meaning is assigned by producers and consumers (ibid). In accordance, such moments are part of culture as discursive practices.

The circuit of culture has also been discussed in relation to technological developments, especially the rise of the Internet within new media studies. In their enquiry of the music file exchange software called Napster, Taylor, Demont-Heinrich, Broadfoot, Dodge and Jian (2002) note that a medium such as the Internet influences the associations between the moments of the circuit. Likewise, the Sony Walkman study (du Gay et al. 1997) is a study of the electronics era and the culture it created. Following and supplementing the body of research laid by Napster and the Sony Walkman, this study will highlight the role of intrusive technologies, specifically spyware, in the digital age, positioning it as the cornerstone to gain an understanding into the cultural implications. However, this theory has a weakness in the sense that it contains an arbitrary nature of nodal points (Leve 2012), and for this reason this research relies on the surveillance studies to reinforce and add depth to the theoretical dimensions, particularly with regards to the issue of online privacy and freedom. To my knowledge no research on intrusive technologies associated with the digital freedom discourse has been conducted in the case of Turkey in relation to the EU.

The corpus of texts collected for this study comprise of normative, symbolic, and political perspectives of digital freedom and intrusive technologies reflected in total of twelve reports; five from the EU and seven from a research institute based in Canada, the Citizen Lab. I will closely read the reports published by the European Parliament and its representatives, which are designed to convey messages to ensure the EU's appeal.

Subsequently, I will evaluate the discourse in a cultural circuit equation mainly through the studies of the Citizen Lab. Together this provides an interesting corpus to describe the dynamic relationship of digital freedom, discourse and the intrusive technologies because every stage of the cultural circuit will allow to view the interwoven practices from various perspectives. With this stance, this thesis will have a critical dimension in as much as it will distance away from taking the statements made by the EU as a whole. I will account for the corpus of the official documents on which this study is based and explain why they are particularly relevant in detail in Chapter 2 where I visit the EU objectives and in Chapter 3 where the implications of spyware technology will be pulled back to a discursive level through the stages of the circuit of culture.

Reflecting on overall content of the intrusive technologies and the key players who are part of surveillance infrastructure, Citizen Lab (2014) reported that the Turkish Government has been able to acquire advanced surveillance technology called the Remote Control System (RCS) from a company called the Hacking Team. This spyware technology works through malware installed on targeted individuals' computers having been sent through the Internet containing a malicious link or a file disguised as something of interest to the individual (CAUSE 2015). The reports have shown that the Turkish government imported these technologies, and how they have been using them is one of the concerns of this thesis. With this regard, the RCS technology will be used as the object of the research, which will also provide useful insights on the discussions surrounding electronic surveillance. However, there is little need to focus on the 'readers' (the users of the technology) as the reports are descriptive texts designed to convey decisive discourses (McRobbie 1978). On that account, the readers were regarded as secondary in the process of creating meaning. By situating my research within the reports indexed throughout the thesis, I aim to contribute to the literature on the cultural value of intrusive technologies, whilst also addressing the EU's current stance in its 'digital revolution'.

In order to understand the extent to which practices and technologies of intrusive surveillance in Turkey corroborate or conflict with the discourse of digital freedom, a perspective that can be used to evaluate discourse needs to be first investigated. Following the introduction, Chapter 1 will signal a cultural view on discourse production that will describe the cultural circuit framework which has been thoroughly used for assessing technologies. Chapter 2 continues to explore state sponsored electronic surveillance and draws out the EU's digital

freedom discourse by capturing the discussions on online privacy and freedom. Chapter 3 will assess cultural circuit of the spying tool, Remote Control System, followed by a discussion. The final chapter briefly re-asserts the key findings of the study and its contribution to both digital surveillance research, and offers some reflections and suggestions for further research. To avoid unambiguity, I would like to note that the intrusive technologies are used for electronic surveillance activities, therefore, the term intrusive surveillance will be used in the same manner. Likewise, spyware technologies will be referred as intrusive tools.

CHAPTER 1: A CULTURAL APPROACH TO DISCOURSE

As this study focuses on the discourse of technologies and practices of intrusive surveillance from a cultural point of view, initially, it is important to touch upon the concepts of culture, knowledge, and power in the context of Turkey in relation to the EU. Through the circulation of cultural meanings, the EU's discourse becomes a *knowledge* within a situated culture (Scott, Bernadette and Wills 2006). In other words, it shows how the digital freedom discourse was produced and legitimized by the EU as knowledge. To illustrate, "the EU provides a digitally free atmosphere" or "the EU fosters digital rights beyond the continent" are part of the knowledge that is profoundly shaped by the EU and which, in turn, shapes the subsequent discourse of digital freedom (ibid). Therefore, the use of cultural circuit research design will enable to explore how the technical and appropriated aspect of the intrusive technology, that is moulded by the Turkish authorities for power, endorse or contradict with the situated knowledge, specifically the digital freedom discourse. To achieve this, this chapter will mainly describe the ways in which a discourse can be examined through a cultural lens, subsequently providing guidance to tackle the research question. From this perspective, I will first explicate how the discourse analysis can be achieved through the moments of the circuit of culture. Then, I will describe why the model makes it useful to approach intrusive technologies for evaluation.

1.1. Language, Culture, Discourse

The discipline of cultural studies seeks to study the role of culture and its relationships to, the production and consumption of everyday life, identity, knowledge and power (Hartley 2003, 3-4). Correspondingly, this motivation signalled a cultural view on discourse. In the examination of discourse, researchers have used the circuit of culture as a guiding framework to consider historical, institutional and contextual factors that affect communication. As

cultural studies accounts for analysing the discourses, this body of work is promising theoretically for how it considers meaning and messages in multiple ways.

The point of departure is Barker and Galasinski's (2001) *Cultural Studies and Discourse Analysis* where they describe how the notion of culture is assessed and has evolved over time. To begin with, culture is examined through its own specific meanings and logic without having scaled down to any other phenomenon such as Marx's "mode of production". The aspects of a social formation that had previously been differentiated from culture can be explored as cultural (ibid). For instance, 'economic forces' can be considered as cultural because they involve a set of meaningful practices, including the social relations of production and consumption. As du Gay et al. (1997) argue, "Rather than being seen as merely reflective of other processes -economic or political- culture is now regarded as being constitutive of the social world as economic or political processes" (4).

Derrida (1976), on the other hand, notes that meaning is inherently unstable and can never stay fixed. It constantly slides away because of its origination through the play of signifiers. As the words carry collective meanings, involving the marks or echoes of related words' meanings in diverse contexts, language stands as being non-representational. To simplify, grasping culture is to look into the symbolic production of meaning through signifying practices of language within varying contexts.

Foucault (1972), like Derrida, is more convinced with the description and assessment of the appearances of discourse and their impacts under explicit material and historical conditions. For Foucault, discourse constructs, defines and produces objects of knowledge in an intelligible way, while ruling out other ways of reasoning as unintelligible. The term discourse "refers to a group of statements in any domain which provides a language for talking about a topic and a way of producing a particular kind of knowledge about that topic" (Thompson 1997, 222). As a result, discourse is perceived as a social practice. Relating to the social world, each discursive event is influenced by social life and embodies new forms of thinking (Carvalho and Burgess 2005).

Moving beyond culture and discourse, for the study of intrusive technologies in the context of Turkey, the circuit of culture has its own semiotic processes of 'encoding' and 'decoding' meanings in verbal and visual texts, confined by contextual factors at its heart (Johnson 1986: 1458: Hall 1973). The main proposition of the model is the supremacy of power in relationships and the connection of culture, knowledge, and power. It is concerned with the ways in which the value and meaning of cultural phenomena are transformed

throughout various sites, moments, and practices (Taylor et al. 2002). Dating back to Marx's 19th-century analysis of the "circuit of capital", which defines the moments of industrialised production and commodity-circulation, (Dyer-Witherford 1999, 91) the model is then collaborated by du Gay et al. (1997). They restructured the model, including interconnected spheres of *Representation*, *Identity, Production, Consumption*, and *Regulation.* As a result, the circuit focuses on how the disparate elements of the moments were temporarily articulated to create functional phenomena (Hall 1973).

The discursive process of constructing and shaping cultural meaning is called representation. Hall (1997) says, "We give things meaning by how we represent them" (3). Production, in a different manner, denotes to meanings related to products, services, experiences, or in the case of intrusive surveillance the messages are deliberately framed for the targeted individuals in Turkey. Consumption is where meaning is completely grasped because "meaning does not reside in an object but in how that object is used'" (Baudrillard 1988, 101). Identities are shaped through the production and consumption process, which are shattered and compounded due to including subjective and socially developed constructs such as power, privacy, freedom and so on (Sarabia-Panol and Sison 2013). Finally, regulation holds the formal and informal cultural control mechanisms that rule the spectrum of social norms, technology and institutions.

In consequence, to evaluate the meanings derived from the discursive aspects, I have discussed how a particular discourse, such as the EU's digital freedom, can be looked through the underlying principles of the circuit of culture. It is evident that every moment in the interdependent cycle of relationships in the model is susceptible to treatment using discourse analysis. Discourse analysis embraces directly with the cultural circuit model given its political aim of placing the form of text, the process of production of text, and the structure of power giving rise to them (Barker and Galasiński 2001). Thus, the theory is useful for understanding the discourses constructed by a group of people and authorities like in the case of the Turkish governments' mass surveillance practices. However, as the studies' main focus is to understand the technologies and the practices of intrusive surveillance in the context of Turkey, one must also enquire into how to make sense of technology using the cultural circuit. For that reason, I will discuss technologies explored through a cultural lens in the following section.

1.2. A Cultural View on Technologies

In the first place, I perceive intrusive technology as a cultural artefact or product that intelligibly shares certain meanings coupled with a distinct set of social practices. Representing a way of positioning from a group of people both to the users and the targets, the technology has acquired a social identity (du Gay et al 1997). Therefore, a comprehensive approach to study spyware technology will aid in understanding its relation to the digital freedom discourse. In that sense, the circuit of culture (Johnson 1986: du Gay et al. 1997) provides a practical ground for the analysis of the technology in reference to Turkey, and for the foundation of the theoretical aspects being applied to this study.

Previously, Stuart Hall (1973) came up with the process of encoding/decoding of the meaning for the television programs. However, the model has not offered a circle back to the encoder. Taking from this account, the circuit of culture later is developed to study how Walkman is represented, what social identities are associated with it, how it is produced and consumed, and what mechanisms regulate its distribution and use (du Gay et al. 1997). Moreover, Julia D'Acci (2004) proposed a circuit of media study, in a similar manner, Taylor et al. (2002) conducted an in-depth examination of a peer-to-peer music exchange called Napster. The Napster study echoed findings about how technologies situated as cultural artefacts and chronicled a conflict of cultures between old and new media. It crucially became the symbolic locus of a multi-perspective struggle "where different discourses alternatively make contact, affiliate, and clash with each other" (Taylor et al. 2002, 614).

Spyware technology as a form of cultural production that is shaped by social structures, likewise is discursive. Specifically, the technology of the Remote Control Systems (RCS) is selected because the medium reaches domestic and cross-national borders and, regarding its use in Turkey, raises conflict. Thus, it furnishes a rich multi-layered site for cultural production. In this respect, RCS is constrained by various discourses that are also a site of challenge as the state may negotiate the digital freedom discourse in its use.

To sum up, this thesis aligns itself with the view that intrusive technology is a ritual form which is "synergistic, nonlinear and dynamic" (Curtin and Gaither, 2005, 93). Considering its application in Turkey at certain stages in the country's history and lived experience, this study will not reflect the empirical–administrative tradition, rather extend the range to social, cultural and political contexts of new media studies (Sarabia-Panol and Sison 2013: Dozier

and Lauzen 2000). It is important to note, intrusive technologies are supposed to be only accessible by the governmental authorities (Hacking Team 2015). Therefore, the issue draws attention to states' interfering with electronic surveillance activities through the Internet, showing us that mass and targeted surveillance achieved electronically by these tools, highlights where the EU objective, Internet freedom and privacy, is at risk. As the focus lies on exploring the discourse of digital freedom produced by the EU *for* and *about* the problem of Internet freedom, the next chapter will evaluate the literature on electronic surveillance and the rhetoric of digital freedom. As I argue in this thesis, studying spyware technology in Turkey through a cultural perspective requires to look into the way it is represented, the social identities ascribed to it, the process of its production and consumption, and the operations that help regulate its distribution and use (du Gay et al. 1997, 3). Spyware technology therefore can be approached analytically as a discursive assemblage that facilitates and orders debates on questions related to digital freedom.

CHAPTER 2: PRIVACY AND FREEDOM IN THE DIGITAL AGE

The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas

— Frank Larue, 2013
Report to the United Nations

The proliferation and intensification of intrusive surveillance practices within Turkey have sparked rich theoretical inquiry, prompted lively debate, and stimulated vital insights into contemporary dynamics of privacy and freedom of speech in the digital sphere (Ball and Haggerty 2005). The purpose of this chapter is to examine this phenomenon by evaluating the notion of electronic surveillance and shed light on the digital freedom discourse by capturing the discussions on online privacy and freedom generated by the EU. The motivation for evaluating the intrusive technology in relation to digital freedom and addressing questions concerning this phenomenon engenders two commentaries: Firstly, it is the aim of this study to illustrate that the state mechanism within electronic surveillance is in line with the relevant theories. Secondly, the digital freedom discourse will be examined by making its entanglements with privacy and freedom in the digital age suspect. This overview will then assist in discovering the apparatus of electronic surveillance, major meanings and qualities ascribed to it, and making sense of the prominent discourse of digital freedom in Turkey, within the broader EU.

2.1. Electronic Surveillance: When Technology Enhances State Power

Cyberspace has now become the global communications and information ecosystem and is immersed in all aspects of society, economics and politics (Diebert 2003). Its distributed architecture has been seen as a basis for a global commons of information, a channel for the flourishing of transnational social movements, and a strong force for democratization (ibid).

However, while these are extraordinary facets of the digital age, the use of Internet in the guise of the finest means of communication has expanded the range and amount of information that can be intercepted and monitored by the governments. Detailed electronic footprints that disclose citizens' behaviours are generated by the transactions conveyed in cyberspace. Therefore, the Internet has also provided an array of means to trace interactivity and to congregate extensive amounts of information both for the governments and private sectors' purposes (Tamara, Massimo, Paul, Christian, Vincenzo and Ilaria 2005). In accordance, discussions about the surveillance of electronic communication have resulted in the dialogues of classical theoretical views in a reassessment of concepts like privacy.

For some theorists who hold a negative view, surveillance is a form of systematic information gathering for the purpose of domination, coercion, or protecting from the threat of violence in order to attain certain goals and accumulate power. Yet in many cases, this is against the will of those who are under watch (Fuchs 2011). In this view, a well-known concept originated by Foucault, surveillance is characterised as a form of disciplinary power. For Foucault, disciplines are "general formulas of domination" (Foucault 1977, 137). The "surveillant Panopticon", a term coined by him, is a machine of power where a person is seen but cannot see, and becomes "the object of information, never a subject in communication" (Foucault 1977, 200). In the Panopticon, discipline crosses a "disciplinary threshold" in which the "formation of knowledge and the increase of power regulatory reinforce each other in a circular process" (ibid, 204). Maintaining control by the constant sense that the person is being watched by unseen eyes, Panopticon presents nowhere to hide and be private in. In this account, using Foucault has unique assets. He illuminates the connections between the Panopticon and state surveillance by showing that it forms the milestone between punitive and reforming disciplinary powers (Lyon 1994, 62). Not only does Foucault situate surveillance as the focus of his theory of disciplinary society but also his portrayal offers a framework for acknowledging "how the architectural characteristics of the Internet likely affect individuals' reaction to surveillance" (Krueger 2004, 441). In this regard, this stance will be useful for the analysis of the cultural circuit of spyware technology in Turkey, namely through the stages of representation, production and consumption. Given the drawbacks of classical surveillance concepts, Fuchs (2011) recaps: "surveillance is the collection of data on individuals or groups that are used so that control and discipline of behaviour can be exercised by the threat of being targeted by violence" (136). With respect to this, the negative

concepts of surveillance that have just been touched upon allow for the drawing of a clear distinction between what electronic surveillance is and is not.

Electronic surveillance— of chat, telephone conversations, e-mails, social media services, Voice over Internet protocol —is now ubiquitous and has tremendous effects both on privacy and freedom of expression and association, and on national security and law enforcement (Podesta 2015). Electronic surveillance is not new, and has a long history as being used as an undisclosed tool for gathering intelligence. During the cold war period, electronic surveillance was globe-spanning and operated in most highly classified domains that were accumulated by the superpowers (Diebert, Palfrey, Rohozinski and Zittrain 2010). However, today's surveillance systems are much more pervasive and are legitimised by tolerant anti-terror legislation that removes many previous operational restraints. They are also increasingly exercised not only by the state but also by the private actors (ibid).

For example, the 9/11 attacks provided justification for the entrance of several new anti-terrorism laws that expanded the government's surveillance powers (Krueger 2005). Legislation has been quickly adopted by many democratic states, creating a more permissive environment that allows for sharing information among domestic law enforcement agencies and foreign intelligence (Diebert 2003, 514). Moreover, the range of potential targets of these new techniques remains uncertain because the state is not obliged to disclose the use of them, combined with the ambiguity of what exactly constitutes 'domestic terrorism' (Krueger 2005, 440). Another ground-breaking incident came into light in June 2013 when Snowden, the former American National Security Agency (NSA) subcontractor started a worldwide debate on the balance between surveillance and privacy (MacAskill 2014) and sparked discussions on the consequences of such large-scale monitoring for individuals' digital rights. The revelations brought into the spotlight not only intelligence and national security agencies' spying practices, but also the suppliers of the spyware industry, which is also a subject matter of this study.

Surveillance theorist Gary Marx (1988) notes in many ways in which electronic technologies foreshadow the 'new surveillance'. Admitting that in some ways the new practices are extensions of technical control, he proposes that electronic surveillance overpowers its limits by moving beyond the intimidating, personalized and non-rational elements of such arrangements, as well as being more intensive, powerful and unobtrusive (Marx 1988: Thompson 2003). Correspondingly, Mark Andrejevic (2005) argues that, in the

age in which every individual is to be regarded as potentially suspect, all are simultaneously urged to become spies. The efficient expansion of power relies on a further asymmetry between observer and observed wherein the latter remains unaware of the extent and duration of monitoring (ibid, 396). Returning back to Foucault, the Panopticon, thus, offers a compelling metaphor for understanding electronic surveillance (Lyon 1994). The prison-like society, where invisible observers track our digital footprints, does indeed seem panoptic. Although, no consensus exists about in what ways and in what contexts might electronic surveillance display panoptic features (ibid, 67), different theorists focus on different aspects of panopticism that reappear or are reinforced by computers. Gordon (1987) believes that we are enclosed in an electronic Panopticon and the effects are societal. Herein the irony is that Foucault himself seems to have neglected the relevance of panoptic discipline to the ways that state power has been enlarged and enhanced by Internet Communication Technologies (ICTs) (Lyon 1994, 67). Though the picture is very similar as the one painted by Foucault, Mark Poster (1990: 1997) portrays a world of consumer surveillance that amounts to a "Superpanopticon" in which subjects constantly produce surveillance data by making numerous cell phone calls, Internet bookings and so on. Occurring in the context of the "mode of information", the technology of power in Poster's (1990) Superpanopticon disciplines its subjects to participate in electronic communications systems which constitute new patterns of language. For Poster (1990), electronically mediated languages represent a new social region distinct from but overlapping with the capitalist economy and the welfare state (Lyon 1994, 85). As an aspect of a new mode of information, electronic language emerges into technically advanced societies, undermining the boundary between public and private space (ibid). However, even if it is panoptic or superpanoptic, no single metaphor is adequate to encapsulate what is central to electronic surveillance. Still, as stressed earlier, important clues are available in the corpus of the texts selected for this study that illustrate the ways in which the contemporary electronic surveillance mechanisms control the marketplace, social life, moral objectives, and surveillance spheres to name a few (ibid). Specifically, throughout the analysis, the Citizen Lab studies will demonstrate how the power of intrusive technologies permeates within relations of the EU and Turkey.

To conclude, the employment of electronic surveillance techniques by powerful actors has acquired a bold and exhaustive character in the last few decades (Verri, Bender and Dondonis 2014). In late 2014 Freedom House reported that "more people were detained or prosecuted

for their digital activities in the past year than ever before" (Podesta 2015). The unlimited power of collecting and processing vast amounts of data increasingly presents as much an instrument as a menace to, particularly, Turkish society (ibid). For that reason, this thesis intends to provoke further thought and reflection upon some of the most fundamental issues surrounding the emergence of intrusive technologies in Turkey as an important topic of investigation.

To this end, it is reasonable to say that disturbances and worries about electronic surveillance arise from some aspects of its panoptic character. To illustrate, electronic surveillance depends upon the characteristics, that no knowledge of the individual is required, that it is increasingly instrumental, that areas of personal life once thought to be inviolably private are invaded, and that it effectively erodes personal and democratic freedoms (Lyon 1994, 78). For that reason, electronic surveillance continually connects with the infringements of the freedom of speech and the right to privacy, which is to a larger extent, concerned with the digital freedom discourse. Having touched upon the issues of state surveillance based on electronic communication, I will now further the discussion on the discourse of digital freedom. To be sure, how closely the current governmental electronic surveillance practices in Turkey or even in European societies corresponds to the promoted discourse of digital freedom remains at issue here.

2.2. Mapping the Discourse of Digital Freedom

The Internet's expeditious expansion has sparked a wide range of debates, nationally and internationally, revolving around online privacy and freedom of expression. Specifically, allegations of the NSA's mass surveillance program revealed the deeply worrying extent to which privacy and freedom of expression are being subverted and jeopardized globally (Pellot 2013). There is no doubt that the practices and technologies of intrusive surveillance have created a conflict between government's lack of trust on their citizens and citizens who do not trust their governments. Today, it is tempting to say that the popular discourse surrounding electronic surveillance revolves around the right to freedom of expression and privacy in the digital sphere as the existing research on surveillance highlights a number of debates primarily about these notions. In *Digital Freedom* Narain D. Batra (2008) notes "For more than a century, privacy has been a matter of grave concern because many new, unobtrusive tools for invading privacy are continuously being developed [..] Big Brother has become a diffused digital omnipresence" (43). In line with Batra, I seek to question the major problems and

beliefs related to this issue that are projected onto the EU's explicit rhetoric on digital freedom. In light of the debate, the European Parliament responds with a formal proposal for new strategy displayed on its website (*europarl.europa.eu*) and four documents published on Marietje Schaake's, who is the member of the parliament, website (*marietjeschaake.eu)*. These communications are not legislative texts to be implemented in national legislation but proposals for policy actions with regards to the issues of Internet privacy and freedom. Although not taken as a whole sale in this study, due to containing proposals for policy actions, the Parliament and its member, Marietje Schaake's, communications have considerable importance to reflect on the EU's rhetoric.

The EU admits that the human rights including privacy and freedom of expression are as crucial online as they are offline, therefore, they have started determining ways to better safeguard these rights (Pellot 2013). One significant development on this front is the EU's work on the forthcoming freedom of expression guidelines, which are to demonstrate principles for promoting and defending human rights more generally in the digital world, both within and beyond the EU (ibid). Following the PRISM scandal about the revelation of the surveillance program that gives NSA direct access to the Internet giants' servers, the necessity for a coherent EU approach to digital freedom has become more critical (Podesta 2015). Director of Campaigns and Policy Marek Marczynski said:

> Crucial decisions will be made that will determine how freedom of expression is regulated online. If the EU is to have a say in how the Internet is regulated and governed, it needs a strong strategy on digital freedom that protects the freedom of expression of Internet users in member states and around the world (Index on Censorship 2013).

Digital freedom has been part of the EU's strategy since 2012 (Schaake 2012). Marietje Schaake's statement on "A Digital Freedom Strategy in EU Foreign Policy" shall now be considered to grasp the EU's positioning on the discourse. The title suggests that the EU attributes responsibility and promises to transform Europe into a 'digitally free union'. Schaake (2012), who has aimed to put the Internet and new technologies on the EU's political agenda says, "The struggle for human rights increasingly has a technological side" and underscores some of the important measures on her report for the digital freedom strategy.

According to the report, unrestricted access to an open Internet is a crucial enabler of fundamental rights and a guarantee for transparency and accountability in the public life (ibid). Another significant matter is to call on support from human rights defenders, civil society activists and journalists using ICTs in their activities and to stand up for their digital rights. Moreover, the report also includes many concrete measures such as that digital evidence, or in Poster's lens electronically mediated language like smartphone pictures and clips of human rights violations, should be permitted in court proceedings. In addition, according to the plan, the EU should terminate the export of intrusive technologies employed by repressive regimes to track and trace human rights activists, journalists and dissidents. Schaake claims that these kinds of exports to countries like Iran and Syria are blocked. She adds, "We need rules and regulations that ensure accountability of companies regarding the impact of their products and software, like misuse for human rights violations. We should think about 'human rights by design' to prevent or limit future harm" (ibid). Furthermore, European Parliament releases another report recently on the issue, establishing counter-terrorism measures being used as pretexts for such violations. As a result, the European Parliament insists that such measures must be pursued strictly in line with the rule of law and human rights standards that consider online privacy and freedom as important aspects (Caponetti 2016). Undeniably, the EU declares that it is undergoing a 'digital revolution' due to its concerns related to protecting digital rights, and achieves to identify itself as the moral guardians (S&D Group 2015). Nonetheless, it is important to note that, besides the ethical considerations, there is a huge economic imperative behind the EU's 'digital revolution', which is the ICT industries' key role in Europe's economic growth and productivity (European Commission 2016). Accordingly, the EU must embrace and disseminate the possibilities, and also promise to restrain the challenges of digital technologies as there is a necessity for the society to engage with them. Otherwise, growing concerns for digital privacy and freedom would only prevent citizens' use of such technologies that have a considerable part in the EU's economy. Needless to say, the interactive networked communication achieved through the use of ICTs always contain an element of privacy invasion and the utilization of such technology allows individuals to let themselves become the forms of asymmetrical and non-transparent information gathering modelled by state surveillance (Andrejevic 2009). However, for the EU, it seems like fostering the use of new technologies ensured with digital freedom is as economically significant as it is for the measures of human rights. Therefore, it is sensible that the EU endeavours to legitimize the *knowledge* –i.e.

"Europe is where the open and participatory Internet is found"- since mapping the digital freedom discourse is closely linked to its industrial systems of *power* (Scott, Bernadette and Wills 2006).

To conclude, in today's world, more countries are turning to cyber warfare where intrusive surveillance becomes omnipresent to accomplish certain goals. In this chapter, to understand intrusive tools' use in Turkey, state-sponsored electronic surveillance has been described and delineated with some of the influential thinkers' perspectives. Thanks to information technologies, Foucault's surveillant Panoptican becomes Poster's Superpanopticon through the obsolescence of digital traces. Examples of this panoptic discipline include monitoring and display of performance data (Thompson 2003, 139) to achieve control of deviance (predominantly reflected as criminality) and novel means of social discipline (Lyon 1994). The discussion then turned to the EU's discourse on digital freedom, which is primarily associated with the electronic surveillance practices regarding its reliance on preserving privacy and freedom of expression in the digital sphere. As this thesis is an exploratory study of digital freedom discourse revolving around the technologies and practices of intrusive surveillance, the examination of these matters throughout the chapter will allow for a clear foundation to integrate the cultural perspective in the next chapter. One of the intentions of this study is to provide an overview of the current state-of-play with regards to the electronic surveillance bearing down on the digital sphere in Turkey. Despite being non-EU, Turkey is a candidate state which needs to comply with the EU regulations and standards including providing a digitally free atmosphere to its citizens. Therefore, taking Turkey as a case, the intrusive technologies will be analysed in light of the reports provided by the Citizen Lab. For the context considered in this thesis, to grasp the form that surveillance may take, I will focus on specific types of conditioning encouraged by the electronic surveillance system through a cultural circuit lens. In doing so, the discourse on digital freedom will be examined by means of the stages where meaning-making is revealed. Consequently, through a close reading of the Citizen Lab reports on the RCS, the next chapter will derive statements from texts in political discourse that can be linked to the digital freedom. This will shed light on the practices and technologies of intrusive surveillance in Turkey, to identify if these corroborate or conflict with the EU's discourse of digital freedom.

CHAPTER 3: CIRCUIT OF SPYWARE

3.1. Turkey: A Look at the Actors and Technology

As RCS technology has been consumed by the Turkish authorities, the Citizen Lab reports on Hacking Team will provide useful insights on the discourses surrounding electronic surveillance. There are currently seven articles from the Citizen Lab published between 2014 and 2016 that will help to investigate how practices, events and social factors are shaped by the relations of power and struggles over power. These texts will be used to reveal representations, identifications, consumptions and productions of intrusive technology that are not necessarily explicit, to disclose the hidden political meanings ascribed to it, and to expose the power relations and dominant actors in the context of Turkey and Europe. To reveal what is indiscernible of the practices of intrusive surveillance, I will also account for *PEN International*'s official document. Throughout the evaluation, the stages will be supported by actual cases that have taken place in Turkey. While analysing the collected texts on the topic, this thesis will assess the situation on the control and use of spyware technology through a cultural level. Therefore, contexts will be addressed both through the reference to key events and characteristics presented within the reports concerning this spyware technology; as well as a more general review of the changing economic, political, and social landscape in Turkey in relation to Europe over the period. My interpretation throughout the analysis is most closely aligned to du Gay et al.'s (1997) cultural circuit with reference to the "overlapping and interconnected elements" through the process of articulation they describe (4). I now start exploring the circuit of RCS by the moment of representation.

3.1.1. Representation

Representation is "the practice of constructing meaning through the use of signs and language" (du Gay et al. 1997, 24). As discussed earlier, meaning is socially constructed through symbolic systems such as language (Hall 1997). In applying this view to RCS, I will resort to du Gay et al.'s (1997) approach with Sony Walkman, which is to understand how new meaning is established through four strategies. First, I posit that RCS is derived from

"something we already know". In this view, the "spyware", "trojan horse", "bug", and "monitoring tool" are existing signs that are transferred in understanding components of the RCS. The literal meaning of "Remote Control System" is already derived from how the technology operates due to its description as an intrusive technology that authorizes cyber investigation (Citizen Lab 2014). Hacking Team utilises this term to capture the law enforcement and intelligence services for applying 'lawful' interception by providing a system that facilitates the digital control.

A second strategy is to associate the object with various discourses. Like many cultural artefacts, RCS's meaning is not limited to literal denotations. To give an example, the RCS is recurrently articulated with other discourses, such as those of "offensive technology", "security", "intelligent services" and "governmental interception" ("Hacking Team" 2013). As a result, RCS has acquired connotations of advanced technology, intrusive surveillance, state interception, advanced infection, and malicious software to name a few. However, RCS is mediated as a device that enables retaliation against the criminals and terrorists. On Hacking Team's website, the technology is introduced as an "offensive security" that "takes control over and monitor targets". Moreover, on a response letter to one of their critics, Hacking Team deliberately used the terms: "legal surveillance software", "legal surveillance technology" or "lawful surveillance" (Privacy International 2016). Their rhetoric clearly mirrors the state's deliberate approach in monitoring the citizens for 'security' purposes or in the name of the law, which is how the company wants to be represented in the public eye. For example, one researcher condensed RCS's intercepting operation as follows: "That's actually what makes it different from the backdoors that hackers were using sort of for the lulz, like 18 years ago when I was opening my flatmate's CD-ROM drive to freak him out" (Citizen Lab 2013). Such use of the term 'backdoor' also invokes discussion for online privacy and freedom that contemporary surveillance mechanisms tend to violate.

Du Gay et al. (1997) claims that "it is difference which signifies" (17) and acknowledges signs as a marker of division. As a third strategy, RCS departs, for instance, from other conventional forms of surveillance technologies such as closed-circuit television. RCS signified because it demonstrates a basic difference in how surveillance is achieved in a digitized form which offers the invisibility of the 'inspection', an automatic character, and the blurring of conventional boundaries.

The final strategy is to articulate meaning through relating artefacts with major cultural themes. Here, the RCS elicits larger discussions about controversial matters, such as the

impact of such technologies on privacy and the freedoms of targeted individuals, and most notably about states' internal dimension involving the surveillance of citizens. RCS's controversy creates social drama because the technology is represented as a device that will be used for targeted surveillance, which means that it depends upon the existence of prior suspicion of the targeted individual or organisation. Therefore, it requires judicial or executive authorization for surveillance (Caponetti 2016, 53). Nonetheless, RCS has been used for mass surveillance practices directed at citizens that grants indiscriminate monitoring of large data streams at a network level where the collection of information is arbitrary (Bauman, Bigo, Guild, Jabri, Lyon and Walker 2014). RCS, therefore, also represents a permanent delegation to evade the law.

Up to this point, I have implemented du Gay et al (1997) and Taylor et al.'s (2002) four strategies of meaning-construction for understanding representations of spyware. To create a more dynamic image, I now refer to Hall's concept of articulations, which involves a "non-necessary set of specific connections formed in the conjuncture of other social forces, practices, identities, and ideology" (Slack 1989, 331). In this view, the articulation of technological meaning is exposed to the dominant power relationship, but it is also composed of reproduction and transformation: "different articulations empower different possibilities and practices" (ibid). With a variety of political and economic influences, the representation of RCS technology constructs a positioning of constant endeavour for the articulation of preferred and oppositional meanings; specifically legitimising the mass surveillance activity by predominantly using the excuse of preventing potential criminal and terrorist activity.

In my view on the representation of RCS, different discourses preferably connect, associate, and clash with each other, creating a symbolic site of struggle. The most common example involves the conflict between governmental officials using it for 'security' purposes whilst giving birth to fundamental threats to citizens' privacy and freedom. The state stands as both the legislator of the spyware trade controls and the guarantor of fundamental freedoms. However, the states' capacity to regulate the digital sphere, as well as their 'security' approach, is arguable vis-à-vis the growing violation of citizens' privacy and freedom (Caponetti 2016, 55).

3.1.2. Moments of identity

Technologies are given identities, which are discursive categories produced at the junction of various attributes, capacities, and forms of conduct at specific historical moments (du Gay et al. 1997). Identities are contrasted around an artefact and through its use, and are attached to both artefacts and users (ibid). RCS, also known as DaVinci or Crisis, is a cultural artefact that is associated with certain social practices, groups of people and social identities. RCS acts as a mark where identity creates meanings and meanings create identity. Here, I will discuss the multiple meanings that constitute identities- not as an object but as a mutable dynamic process (Motion and Leitch 2002, 52).

Hacking Team, as the creator of the "lawful interception" trojan known as RCS, prompts meanings through every action or inaction, every statement or silence. According to the Hacking Team, RCS is considered as a necessary and legitimate instrument for the 'legal' surveillance of the Internet and telephone data for the purpose of law enforcement and crime investigation. In constructing this identity, sad but true, Hacking Team's statements reflect the vision and aspiration of the Turkish government who intensely increased the capacity for mass surveillance (hereby will be discussed specifically in the regulation section) (Shaw and Sentek 2016). Resembling that of oppressive states, the Turkish government has been wrestling with the tension of the relentless drive to employ new technologies that will flow with their power and authority (Diebert and Rohozinski 2010, 3). As states seek to normalize control and exercise power through new technologies (ibid), the spyware industry has allowed to equate technology with empowerment. Therefore, the Turkish government can 'legally' spy at the key points of the Internet infrastructure to maintain the control against power threats.

On the other hand, RCS's 'ethical' identity is certainly not shared by the EU. Unlike the producer-defined identity of RCS, the EU acknowledges this technology as a 'digital weapon' that causes serious damage to fundamental freedoms, namely the right to privacy and data protection (Caponetti 2016). Whilst the founder of Hacking Team asserts that they do not trade "weapons, [and] do not sell guns that can be used for years", the United Nations including the EU, insists on considering Hacking Team's RCS as belonging to the category of "military assistance" (ibid, 61). To be sure, Hacking Team, likewise 'powerful' states, will continue to negotiate the product's identity as the defender of security.

Nevertheless, in Turkey, the legalised spy kits often appear to point in the opposite direction. To illustrate, the Turkish governmental officials and then-Prime minister Erdoğan, who was locked in a power struggle with religious cleric Fetullah Gülen, was targeted by their

own digital weapon in wiretapping corruption scandals on December 17, 2013. Though political tensions got stirred by the recordings, the conversations were described as a shameless 'montage' to the Turkish society (Nakhoul and Tattersal 2014). Erdoğan and his supporters soon established a new identity called 'parallel organization' referred to those whom walk with the Islamic cleric Gulen claimed to be responsible for the wiretapping scandals. Therefore, montage as an excuse not only facilitated the internalisation of the 'parallel' identity, but it also had little effect on Erdoğan's popularity and power.

Consequently, while the invasion of privacy and freedom discourse continues to underpin its implications, Hacking Team has extended its scope to implement identities such as 'lawful' interception, enhanced 'security' and 'ethical' hacking. Here, I explored a paradoxical identity configured around the RCS technology within Turkey. Considered as 'digital weapons' by the EU, spyware technology has created complications within the Turkish government in terms of its use by the 'parallel' forces inside the government officials.

3.1.3. Production

In the simplest way of describing production is that it is both material and cultural and involves the basic creation of goods and services, as well as of cultural meanings (du Gay et al 1997). Production provides an answer to what meaning is injected into a cultural artefact, and who creates this meaning (ibid, 3). It involves having to consider "a number of different narratives and representations of the 'facts' that have become associated with the technology" (ibid, 42). RCS goes through a production process where certain meanings are ascribed. Through encoding process, RCS translates various ideas into social practices, and therefore, the company, governments, and others who are involved, all contribute to how this technology is interpreted in society. By focusing on the processes of production of the RCS, I will now examine the meanings imbued in the technology.

In analysing Napster's culture of production, Taylor et al. (2002) mainly address its representations. The representations of RCS that I have discussed above, presumed to reveal wider sets of cultural relationships, namely the state's digital espionage and digital freedom of targeted individuals where the technology is entangled. Moreover, they argue that consumption is the most critical element in articulating production as it fulfils the intentions of producers to make products that are 'useful' and effective (ibid). In this stance, I begin by accounting RCS's status as an intrusive software. In contrast to conventional surveillance techniques, RCS transpired in the digital age, generating an alternative for the practices of

electronic surveillance. The RCS tool is capable of recording text and audio conversations from Skype, Yahoo Messenger, Google Talk and MSN Messenger, including other communication applications. It can also steal Web browsing histories and turn on computers' microphone and webcam to record conversations and even take photos (Zetter 2013). Therefore, the way RCS is designed produces an act of meaning, which is as explicit as it is seen, a tool for extensive intrusion.

As mentioned earlier, the cultural circuit focuses on the ways in which the values of cultural phenomena are created. At this stage, it is therefore appropriate to give due consideration to RCS's concept of value and its formation. Throughout the circuit of RCS, not only is money being circulated in the exchange relationship but also social and cultural meanings and messages. Regarding material production, the distribution of surveillance technology has emerged as a 21st century arms race (Citizen Lab 2015). According to Ron Diebert from the Citizen Lab, the trade of intrusive technology involves several actors: the professionals, the big firms that are very legitimate like the Hacking Team, and the unscrupulous part of the business that is covered in secrecy (ibid). He adds that in the surveillance business, the private sectors are involved very little with government regulation. As the private sectors are naturally concerned with profit maximisation in the absence of government regulation, it is reasonable to see firms like Hacking Team expanding their reach and claiming that they only "sell to law enforcement and intelligence agencies and will not sell to countries that are blacklisted by NATO" (ibid: Jeffries 2013). However, the intensifying reliance of governments on the private sector, which seems more capable of keeping up the pace with technological changes and demands, also becomes instrumental in the growth of the sector (Caponetti 2016). These technologies have started to be seen in the context of a global market that has been growing by 20% annually and back in 2011 it was estimated to be worth between 3 to 5 billion dollars by industry representatives (Silver 2011). Assuming that now the market has grown even more, this response echoes viewing value through the Marxist traditions of 'use' and 'exchange' value whereby monetary exchange takes place and represents the potential of the advanced technology to accelerate capital's eager quest (Taylor et al. 2002, 618).

As value is not just economically determined according to Marxist tradition but culturally constructed, I now place my focus on the concept of value where spyware technology is not just considered in monetary terms alone. Today, Hacking Team's flagship product, RCS, enables law enforcement at federal, state, or local levels to collect heaps more

data than the NSA's controversial PRISM and yet they are reluctant to introduce necessary safeguards to minimise the information that is collected (Jeffries 2013). With the lack of existence of prior suspicion to use this technology, the bulk access to all digital communications traffic leaves considerable doubts concerning the violation of many citizens' privacy and the grant of power that comes with unaccountable surveillance. Therefore, money is not solely exchanged by Hacking Team, so is the emerging configurations of power and influence, as there are practically no limits on what governments can do with this broad access to continue maintaining the surveillance superstructure.

Hacking Team, who used to be a small tech security consultancy, in time, ended up transforming into one of the first sellers of commercial hacking software to the police (ibid). The Milan-based company now has many employees and sells intrusive hacking software to law enforcement agencies in many countries (Citizen Lab 2014). Nonetheless, Hacking Team who has frequently sought to represent itself to the world as an ethical company is not the only firm actively in charge of producing spyware. Indeed, companies in Finland, Sweden, Denmark, Ireland, United Kingdom, France, Germany and Italy developed surveillance technologies, especially the companies Gamma, Trovicor and Amesys stand as the strongest actors (Wagner and Bronowicka 2015, 154).

The role of the EU-based companies is recognised as having an important share of the global market in ICTs, particularly in the field of intrusive surveillance, therefore, clearly identified as having contributed to human rights violations worldwide through the export of such technology (Caponetti 2016, 69). Although the EU acknowledges this phenomenon as an issue that needs to be resolved, the root of the problem is to allow these countries to extend their scope and power in time, and let them build a disruptive infrastructure at first. To be sure, the EU poses a 'strong' strategy as a rhetoric on protecting digital freedom since 2012. There is however, still an increasing concurrence that the EU should re-evaluate its export control measures to bring them aligned with its rhetoric of protecting digital rights not only in Europe, but also in other countries, because the amount of the EU-based surveillance technologies sold abroad without licensing is expanding (Wagner and Bronowicka 2015, 154-155). Moreover, the EU tends to criticise repressive countries for violating human rights, which poses a controversy as the tools that have been consumed are those produced by the European countries (ECDHR 2016). Therefore, in my opinion, the EU's act and amount of meaning making of RCS is problematic since it challenges its own dominant beliefs and values, specifically the ones that address digital freedom.

To sum up, even as it is formed a threat to the established digital freedom strategy, RCS technology continues to expand its circle of production to match the growing volume of consumption. Though the EU aims to promote a 'digitally free' atmosphere and also acknowledges the export of these technologies posing threats to human rights in certain countries, it has allowed and still continues permitting firms like Hacking Team to transform other countries into a digital gestapo. Simultaneously RCS represents power as the cultural value for certain states, and the relentless expansion of capitalism due to the huge economy circulated thanks to the so-called "online security" firms.

3.1.4. Consuming RCS

Goods are "produced in ways that make them meaningful" but are also meaningfully incorporated into our daily lives through consumption (Acosto-Alzuru and Kreshel 2002, 143). RCS has the identity where specific patterns of consumption communicate social and cultural characteristics (du Gay et al. 1997). Accordingly, like a language communicating who we are, consumption is seen to constitute systems of signs and meaning (ibid). These constructions of meaning are not displayed in the artefacts themselves, but in the practices of consumption. To illustrate, advanced surveillance technology can communicate the ability to have control over others, which can be referred as signifying practices that serve to connect products with certain meanings and values (ibid). Hence, meanings incorporated in artefacts are interpreted differently by different people according to their norms, values, tastes and opinions.

An important theme to the RCS narrative is the various connections that have been established. In July 2015, the Italian company Hacking Team itself was hacked, resulting in more than one million e-mails and many administrative documents stored on its servers being leaked to the public (Citizen Lab 2015). The company has repeatedly been exposed for selling its highly intrusive spyware to oppressive regimes although claiming otherwise. 400 GB of documents that were leaked were the list of the company's active and inactive clients. Among the company's clients, needless to say, there were police and state security organisations in repressive countries, and police agencies and companies in several European countries (Batey 2011: Bryant 2015). This clearly shows certain groups like European police forces have neither interpreted nor incorporated the EU's objectives as they have been consuming the products ascribed as 'digital arms' by the EU. Purportedly the hacked

documents revealed that Turkey was one of the major customers of Hacking Team. Turkey's civilian police force, the General Directorate of Security (GDS), contracted with Hacking Team to use the RCS product from June 2011 to November 2014, and paid $600,000 to spy on its citizens -as specified by scholars- this is likely illegal practice (Sözeri 2015).

Turkey has been hosting RCS activity for years. In 2012, experts detected twelve cyber-attacks by RCS tools to five separate targets (Golovanov 2013). Citizen Lab's 2014 report lists 10 IP addresses of servers from Turkish ISPs that have the fingerprints of Hacking Team's fake security certificates. One of the endpoints noted by the Citizen Lab researchers as a "spyware's government operator" was a server owned by Turkey's largest ISP, Türk Telekom, where the team detected activity for a week in November 2013. Although, the exact targets of the Turkish police force are still unknown, the cumulating evidence provided by the report indicates unlawful purchase of RCS tools paid by Turkish taxpayers, and targeted spying on its citizens by then-Prime Minister Erdoğan's command (Sözeri 2015). However, now the consumption of intrusive surveillance does not just intend to cover so-called enemies of the state but a far wider portion of society. Referring to the December 17 corruption scandals, investigative journalist İsmail Saymaz notes, "In a country where the prime minister says, 'They even listened to me!' Who can judge the man who runs the corner store from feeling afraid, from asking why the powers that surveilled the prime minister wouldn't surveil him?" (PEN International 2014, 44).

As a result, a handful of surveillance scandals that have rocked public confidence have given rise to a common impression that those who are engaged in completely legitimate activities are subjected to surveillance with far too much ease (ibid). These concerns were boosted because of the previous misuse of digital and telephone records to incriminate journalists and other writers in infamous Ergenekon[1], Koma Civaken Kurdistan (KCK)[2] and OdaTV[3] trials, and Turkish Intelligence Agency (MİT)'s use of fake names to acquire and renew surveillance orders against journalists (ibid, 43). Even more worryingly, to implicate writers and journalists, digitally fabricated evidence has been used in these trials. Occurring in the context of Poster's (1990) mode of information, new individuals are created who carry the same names but whose activities are built artificially from matched data. The citizens, namely

[1] High-profile trials in which 275 people were accused of plotting against the Turkish government

[2] Turkish authorities' suppression on pro-Kurdish voices whom they alleged were associated with the KCK, which is claimed to be an umbrella organization of Kurdish Workers' Party (PKK)

[3] Oda TV were accused to be the media arm of Ergenekon organization

the journalists, become intimidated and frightened because the intercepting and monitoring activity poses fundamental threats to their freedom of expression, freedom of thought and privacy. More importantly, none of this is applied in a transparent manner or in compliance with the law. Therefore, there is no limit to the state's perpetration to silence a dissenting voice, or overshadow journalistic activity that does not suit the Turkish government's interests. Here, the Turkish government's consumption of intrusive technology does not fit in the digital freedom schema. An academic and political analyst who was arrested on suspicion of entailing in the Oda TV case, Coşkun Musluk, in an interview with PEN International (2014) says:

> They took my columns, the emails I wrote to journalists, the messages I sent to my girlfriend, my entire address book (including everyone's names and numbers) and even a conversation I had on Instant Messenger; and put these in the court documents. They put them under the "activities committed in support of the Ergenekon-controlled, armed, terrorist organisation PKK" section and in the appendices. Regardless of the fact that none of this constituted anything like proof of criminal activity. They then picked and chose excerpts from these to put in the indictment.

What makes this issue even worse is that the state's mass surveillance activity is used to profile individuals for their political and ideological beliefs to render them susceptible to persecution, thus, leading to intensified self-censorship of individuals. Subsequently, in a society where government officials have access to citizens' personal data collected on the systems through the intrusive tools, citizens exhibit conformity which seems to be a case of Foucault's (1977) disciplinary power of the panoptic or, in the contemporary landscape, superpanoptic. In both ways, state, in a manner of disciplining the subjects, crushes the distinction between private and public life by monitoring or even fabricating personal data of the most mundane and intimate kinds.

According to du Gay et al (1997), an object's meaning is not determined solely during production but is instead subject to an impact of consumption patterns. Despite the producers' effort to elicit the use of RCS as a legitimate act of spying on criminals, the way the Turkish government consumed the product diffusing into the society at large is completely inconsistent with how it is represented. Given the operational concerns with electronic

surveillance in Turkey outlined above, it is important to note mass surveillance practices –not as extreme as it is in Turkey though- have also been taking place in European countries. As the recent revelations by the whistle-blower Snowden exposed mass state surveillance by European governments including the UK and France (Greenwald 2014), the EU once again is caught up in paradox. Even though the revelations then have accelerated the EU's intention to protect digital rights, it has not prevented European police forces to continue buying RCS products from the Hacking Team.

3.1.5. Regulation

Conceptualising the moment of regulation explores the attempts to control cultural activity. In du Gay et al.'s (1997) lens, meaning is shaped for the attempts to regulate the production and consumption and use of the artefact, but also for the "impact [RCS] has upon the regulation of cultural life" (144). RCS is particularly a compelling technology that has been subjected to intensive legal regulation to either facilitate or to prevent its consumption. Here, I will emphasise these regulations to show how dominant actors have re-articulated the production and consumption of RCS through policies. Despite the growing concerns about mass surveillance, meanings surrounding the regulation of RCS reflects the play of power, in other words, it is dominated by the logic of capital.

In the realm of regulation, some legislation has been passed in Turkey following the 17 December 2013 corruption scandal that severely threatened the digital rights of many Turkish citizens. Firstly, the law that gives National Intelligence Agency (MİT) wide-ranging powers to conduct surveillance and collect information entered into force on April 2014 (PEN International 2014, 42). Secondly, on 3 April 2015, a hotly debated bill known as the Internal Security Package, which was widely criticized by oppositional parties and many citizens, was introduced to the parliament, containing very worrying provisions that empowered the police. The law also expanded the length of time for the police force to conduct digital surveillance on individuals who are "suspected of national security offenses without requiring judicial authorization" (ibid, 43). Furthermore, it permits the police to solicit information from telecommunications companies to locate, monitor, record and evaluate conversations in 'urgent cases'. This clearly shows how the state requires telecommunications providers to make the networks compatible for electronic surveillance by applying and enforcing 'lawful interception' standards (Gutwirth, Leenes, Hert and Poullet 2012).

In addition, in the absence of data protection legislation, the Turkish government requires SIM cards to be registered as mandatory, therefore, simplifying communications surveillance and interception (ibid). Besides, aiming to harmonise Turkish legislation with European conventions and directives, a draft law concerning data protection, has been in the pipeline for over a decade now. However, the aim of this new law was not just protecting the personal data from commercial sales, rather opening up the vast amount of information to the state (ibid). Finally, the terms of, again, the highly disputed Internet Law asserts that ISPs are prohibited from monitoring information that goes through their networks, and are not obliged to seek out illegal activity. However, it lacks the provisions to ensure accountability and the protection of privacy.

It is apparent from the above that, Turkey's regulations enabling the practices of targeted and mass surveillance, likewise the use of RCS, does not comply with the EU's obligations under digital freedom to respect the right to privacy and freedom. The construct of the Turkish legislation takes for granted a particular modality of power in which implementation and control of the citizens' "electronic collar" are exerted in a top-down way (Anderejevic 2009). Aforementioned legislations, again, help Turkish government constituting a system of surveillance "without walls, windows, towers or guards", in other words, Superpanopticon (Poster 1990, 93). On the other hand, although some European countries have implemented regulations mirroring Turkey ("Mass Surveillance in the European Union: Communications and Financial Transactions" 2016), the EU has been striving to counter-regulate to prevent the range of digital issues undermining citizens' rights to privacy and freedom. However, how well the EU is achieving this is questionable.

3.2. EU as a 'Global Player' in the Digital Freedom

Choosing RCS as the object of the study, I have used the circuit of culture model here to assess the practices and technologies of electronic surveillance in Turkey in relation to the digital freedom discourse. My interpretation was closely aligned to du Gay et al's (1997) framework referring to the overlapping and interconnected elements. It appeared, justifications to stricter surveillance do not need to have links to any crimes in Turkey but even peaceful activism and deviant behaviour. Day by day, citizens are treated as an increased threat to society and spyware tools are used to estimate the level of threat. Although the use of these technologies is

identified as 'lawful interception', it may pose conflicting representations whereby various discourses clash, specifically in terms of the technology's representation as a tool for citizens' security in relation to its actual use; namely mass surveillance.

In the digital era, it is possible to see the Turkish power-holders being targeted by the 'digital arms' technologies themselves legitimised. For instance, despite being ideologically similar, the political tensions between the ruling Justice and Development Party (AKP) and the Islamic community led by Fethullah Gülen have become even more intensified by the engagement in such technologies. To specify: the use of wiretapping in the corruption scandal, by the same token, the revelation of Whatsapp messages of military officers involved in Turkey's recent attempted coup intercepted through a 'security flaw or backdoor' (Davis 2016). This clearly indicates that the government officials whom used to be allied, can even point the digital weapon against each other if they have enough power to access the resources. In this view, perhaps the digital sphere conforms poorly to Foucault's ideal Panopticon or even Poster's Superpanopticon whereby, still in the context of mode of information, the watchdogs cannot at any time be under watch without notice. While this issue is somewhat beyond the territory of this thesis, it became evident that panoptic logic is present in Turkish society in terms of the embeddedness of power in electronic technologies through their consumption and regulation that in turn also generates mode of discipline. Again, the system can be perceived arguably more panoptic due to the citizens' awareness following the surveillance scandals, or the leaks related to intelligence agencies' agreement with the Hacking Team. However, the Panopticon offers no neat description of electronic surveillance as the adoption of electronic communication did blur the distinction between surveillance spheres in Turkey that has always employed an official rhetoric of providing 'security' to its citizens. As a result, either used in a (super)panoptic manner or not, lawful interception technology becomes controversial when states use it as a tool to commit crime rather than suppress it. For Turkey, interception can be used by government officials to secure power, not to prevent crime but to control behaviour.

Sadly, the reach of the spyware technologies is only getting escalated. In fact, the ongoing debates have not hurt the industry, but instead created more demand (Bryant 2013) resulting in global expansion of surveillance societies. Still, at the supra-national level, EU Member States are more engaged to the right to privacy and protection of personal data by the Charter of Fundamental Rights (CFR) of the European Union (Caponetti 2016). Some of the EU's member states are amongst the world's best for protecting online freedom (Harris 2014).

However, these implications merely demonstrate a snapshot of the issue, and the European states ranked as 'free' fall short to wholly sustain their commitments on privacy and freedom of expression. To name a few, through the Snowden revelations, which has caused "serious damage to the credibility of the EU's human rights policy and has undermined global trust in the benefits of ICTs" (Falkvinge 2015), the Guardian reported that mass online surveillance and wiretapping has been carried out by the spy agencies in Germany, France, Spain, and Sweden (Greeenwald 2014). Moreover, Britain's electronic surveillance centre GCHQ was uncovered to play an influential role in aiding countries across the continent to circumvent laws that restrict spying activities. The report said that "Europe's intelligence services had forged a loose but growing alliance," carrying out electronic surveillance (Deutsche Welle 2016). Indeed, following the Snowden leaks on mass surveillance programmes, many European states undertook inquiries and adopted measures which were meant to regulate the use of mass surveillance technology. It appeared, however, that spyware technology used by security and law enforcement agencies, in order to fight terrorism, was not always used in accordance with the principle of proportionality and necessity, giving birth to the phenomenon of mass surveillance to the detriment of targeted surveillance subject to prior judiciary control (Caponetti 2016).

More importantly, at a time when European countries are loudly condemning Turkey and repressing countries for spying activities, Europe's spyware industry is a potential source of embarrassment (MENASOURCE 2015). The legal framework has been left deprived of adequate instruments to control the export of such technologies. As a result, the consequence has been the rapid development of a private industry in supplying such technology to governments all over the world (Caponetti 2016, 70). Privacy activists and politicians worry that, European surveillance technology sales could infringe human rights overseas, as well as be damaging to the cyber security of people in Europe, if left unregulated.

In the realm of digital freedom, the EU has aimed to make positive contributions offering practical measures that are more inclusive of a 'human privacy' approach. Since 2012, the EU widened the scope of its trade control system including goods and technologies named "Intrusion Software" and "IP Network Surveillance Systems" (Wagner and Bronowicka 2015). Despite this improvement, a number of concerns remain that are questionable about the effectiveness of trade controls in prohibiting the breach of human rights, and the volume of trade control systems to employ the human privacy approach. In her study, Lia Caponetti

(2016) discovered that the dual-use nature of software technology plays an increasingly important role in enabling and ensuring the fulfilment and full respect for digital rights. However, at the same time, the same tools can be used for violating digital rights through jamming, interception, unauthorized access to devices, and tracing and tracking information of individuals (ibid, 69). Therefore, the nature of the existing multilateral control regime is an issue as a 'limited' way of controlling the export, transit and brokering of dual-use items, which are the key instruments contributing to international peace and security. Yet the possibility and implementation are up to the Member States.

Another issue concerns the suppliers of intrusive technology that given their duty as states' suppliers, consider themselves "above the law" and refer to their role as "security providers". There is a privileged relationship of the private companies such as Hacking Team with their governments that may not be a guarantee of fairness and "legitimacy, besides their operation being in a grey zone where surveillance technology has not always been clearly subject to trade controls", or under strict and transparent regulation (ibid, 71). Hacking Team, for instance, has been blamed of violating European sanctions due to exporting spy tools to repressive countries as the Italian competent authority issued them a global authorization that allows the company to export RCS freely to all countries. This issue again calls into question: Why would the state give a penalty to a firm for trade controls violations, whereas it is the same company's consumer?

In conclusion, there is no denying that whilst the EU plays a positive part in the global debate over the electronic civil rights for accessing information and the free use of information with no risk to privacy; these requirements are no more fulfilled due to the hacking technologies' global production and spread in the digital arena. Taking a candidate country, Turkey, as a case, the cycle of RCS technology that evaluates the practices and technologies of electronic surveillance has shown that the Turkish government has developed regulations in ways that overstep protecting digital rights and there is no consistent approach to the EU's contradictory digital freedom strategy. Accordingly, these technologies and their practices should be identified, grasped and their social influences should be estimated. Particularly in political decision-making, it is essential to regulate the tools for mass surveillance so that the power-holders are not utilising them to track the activities of dissidents, human rights activists, journalists, students, minorities, political opponents or even the entire population. However, in this case, regulating mass surveillance technologies is not solely the answer. The

dual-use nature of trade control system of technology also poses potential harm to human rights issues because of the obscurity of what is and is not considered as “cyber-tool” or “smart security”. It is therefore important to ensure that the use of such technology is responsible, acceptable and proportionate application in a way that fundamental human rights are still valued.

CONCLUSION

Rapid advancement in digital technologies has also raised new questions around individuals' online privacy and freedom. Acknowledging this complication mainly caused by the electronic surveillance practices, the European Union (EU) implements a discursive strategy, calling it "digital freedom". Aiming to provide insights on the intrusive technologies (tools that are mainly used for electronic surveillance) and their relation to the EU's digital freedom discourse, this study focused on Turkey as a case. Moreover, the spy tool named the Remote Control System (RCS) was chosen as the object of the research. In the course of this, the following research question was central to this thesis: To what extent do the practices and technologies of intrusive surveillance in Turkey corroborate or conflict with the discourse of digital freedom in relation to the EU?

In Hall's (1997) lens, technologies are cultural artefacts. In that sense, du Gay et al.'s (1997) theory of circuit of culture turned out to be practical for evaluating the Hacking Team's well-known intrusive technology, RCS, and determining the surrounding discourses that are constructed by a group of people and authorities. Understanding the technology goes through a process where the meanings are produced and circulated at different sites. Therefore, an assessment was achieved through cultural circuit and made contextually relevant as a tool of analysis that opens the way for an exploration of the multiple interrelated processes involved in the use of intrusive technologies in Turkey. RCS was approached analytically as a discursive assemblage that facilitates and orders debates on questions related to digital freedom.

Spyware technologies, including RCS, however, are accessible only by governmental authorities. This issue raises questions on national states' interfering with electronic surveillance activities, resulting in a direct contradiction with citizens' digital rights. Electronic surveillance and national engagement in such practices were explored through some influential thinkers' perspectives. For some theorists, surveillance is the collection of data for the purpose of controlling and disciplining behaviors of individuals in order to attain certain goals and accumulate power (Foucault 1977: Fuchs 2011). In today's world which is

characterized with the accelerated development of electronic communications, escaping from the gaze of surveillance becomes very difficult since we leave chains of digital records in whatever we do. Whilst Foucault calls this an act of disciplinary power (surveillant Panopticon), in Poster's contemporary lens it is Superpanopticon. From this perspective, the intrusive technologies operate in a (super)panoptic logic where citizens are observed, monitored, and disciplined under the governmental institutions. Therefore, to a larger extent, state sponsored electronic surveillance connects with the infringements of the online freedom and the right to privacy. Drawing on this phenomenon, the EU's Digital Freedom Strategy was delineated to identify the major meanings ascribed to the discourse. It became apparent that, the discourse of digital freedom revolves around protecting freedom of expression online, respecting privacy, and guaranteeing a transparent and open Internet. The focus on legitimizing the *knowledge* of digital freedom also rings true in the EU's industrial systems of *power* in which fostering the use of digital technologies is as economically significant as it is for the measures of human rights. Although it could be argued that the application of digital technologies encourages the extension of surveillance or instrumental discipline, the EU claims to take further steps to employ principles preserving privacy and freedom in the digital spheres. All in all, these principles strive to reflect upon the EU's explicit rhetoric, which was further assessed through the cultural circuit of RCS.

As a result, the analysis of the RCS was conducted in light of the texts comprised of Citizen Lab's reports supported with the actual cases. The findings can be sketched as follows. In the moment of *Representation*, RCS is portrayed as a tool for "legal surveillance". States legitimize its use for security purposes that aims to prevent potential criminal and terrorist activity. However, regarding the issue, different discourses clash in representing RCS, especially the ones that are concerned with citizens' online privacy and freedom. Supposed to be a tool for targeted surveillance, RCS rather gets caught in the friction of being used for mass surveillance. Concerning *Identity,* RCS has been acknowledged as 'legal', 'ethical' and 'lawful' tool for surveillance by the manufacturer, Hacking Team. Though Turkish government recognizes the technology in the same manner, RCS falls short in maintaining its identity in the context of Turkey. To maintain power, the Turkish government tends to alter the identities ascribed to the technology. For instance, in the corruption scandals, authorities asserted wiretapping as a shameful act and whom got involved in using such intrusive technologies ('digital weapons' according to the EU) are identified as 'parallel'. The moment of *Production* of RCS, however, is where the conflict is created in terms of the the digital

freedom discourse. Almost all companies who are in charge of the production of intrusive technologies, including the Italian Hacking Team, are based in Europe and, in time, expanded their scope to match the increasing demand for consumption despite the EU's efforts for the exports control. Through the moment of *Consumption*, it became apparent by the Hacking Team's leaked documents that the European based company has been selling RCS to repressive regimes and to their main customer, Turkey. Purportedly hacked documents also revealed that some European police forces and companies were among the clients who were consuming the products. When thinking of European objectives, this issue is very controversial considering the damage intrusive tools can give on human rights. Indeed, resembling that of superpanoptic practices, the Turkish government has even used these technologies to fabricate data for profiling individuals and for suppressing political dissidents. Finally, in the moment of *Regulation,* Turkey passed legislation that facilitates the use of intrusive technologies and therefore, severely threatens citizens' digital rights.

In terms of the digital freedom debate, Turkey certainly does not comply with the EU objectives. Nevertheless, what we all concurrently recognize, the digital freedom as being part of the "EU objectives", is also hypocritical. Besides constructing particular moral images and appearances, the EU has left their legal framework deprived of the adequate measures to sustain digital rights across and beyond the continent. Specifically, the EU fails to control the export of software technology and to disregard the suppliers of such technology as "above the law". The study also revealed that it is rather hypocritical of the EU to let European nations utilize their private companies' tools but claim to restrict their use to wider market.

More importantly, the circuit of culture model was practical for discovering the bottom of the iceberg, in other words, to understand what is underneath the digital freedom, and to shed light onto how the EU's digital freedom discourse participates in systems of knowledge and power. While some of the knowledge ("the EU fosters digital freedom") has been articulated and legitimated, other possible knowledge ("the EU is the pioneer for creating human rights violating tools") has been marginalized or left silent. Providing a theoretical basis for recognizing that "power produces knowledge", Foucault's (1977: 1980) vision on surveillance mechanisms helped to evaluate certain assumptions. First, in a market economy that depends very much on consumer spending, it is a matter of power for the EU to provide as much intrusive tools as possible, while preserving its 'ethical' identity as the global promoter for digital freedom. Secondly, Turkey, as being one of the major consumers of this technology, often struggles to maintain the panoptic structure of social control as the

government authorities have frequently faced electronic surveillance themselves. With this stance, although it has been argued that we, society as a whole, function as a giant (super)panoptic mechanism (Lyon 1994), consumers of the intrusive technology, the government officials in this case, time to time find themselves in cells at the periphery. The issue of watchdogs being under watch takes 'new surveillance' to a new level for which the illustrative parts of (Super)panopticon are inherently limited.

Returning to the main argument, in a sense, digital freedom has become a conflicting discourse in Turkey, as it is also in the EU. In fact, digital freedom becomes a false promise when thinking in terms of the EU's weak regulations and the Member States' production and adoption of intrusive surveillance tools. Intrusive technologies rely on an extensive European infrastructure that enables their operation. Specifically, the dual-nature of technologies allow intrusive tools to enter the market under the classification of security software tools. Still, considering the damage they cause, the dissemination and use of these technologies are enough to overshadow the EU's explicit rhetoric on digital freedom.

Aiming to extend the existing state of research in the context of digital surveillance in Turkey, this study intended to add a better understanding of the role of intrusive technologies and the way they create a threatening environment for extended data collection without the citizens' awareness. By analyzing the technology in Turkey and within the so-called digital revolution in Europe, the evaluation in the cultural circuit equation intended to add a new way of rationalizing the architects of "security software". The major limitation to this study was the difficulty to access information concerning the state consumption of spying technologies, which can only be acquired by the leaked documents that are displayed in the reports. Therefore, the possibilities for further research go beyond the concrete measures, such as to closely review the regulations for strengthening the control of production and export of intrusive software both domestically and internationally. It is important to prevent the victimization of non-criminal individuals who are the citizens of European and also non-European countries like Turkey. Additionally, more attention must be paid on the digital surveillance practices particularly in Turkey as they are getting escalated and have been a neglected subject of research in the field of new media.

REFERENCES

Acosta-Alzuru, Carolina and Peggy Kreshel. 2002. "I'm an American girl...Whatever that means. Girls consuming pleasant company's American identity." *Journal of Communication* 52(1): 139-161.

Andrejevic, Mark. 2005. "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance." *Surveillance & Society* 2(4): 479-497.

———. 2009. "Critical Media Studies 2.0: An Interactive Upgrade." *Interactions: Studies in Communication & Culture* 1(1): 35-51.

Ball, Kirstie S. and Kevin D. Haggerty. 2002. "Doing Surveillance Studies." *Surveillance & Society* 3: (2-3).

Barker, Chris, and Dariusz Galasiński. 2001. *Cultural Studies and Discourse Analysis: A Dialogue on Language and Identity*. London: Sage.

Batey, Angus. 2011. "The Spies behind Your Screen." *The Telegraph,* November 24. Accessed July 15, 2016. http://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html.

Batra, Narain Dass. 2008. *Digital Freedom: How Much Can You Handle?* Rowman & Littlefield Publishers.

Baudrillard, Jean. 1988. *The Ecstasy of Communication*. New York: Semiotext.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and Rob B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8(2): 121–44.

Brivot, Marion, and Yves Gendron. 2011. "Beyond Panopticism: On the Ramifications of Surveillance in a Contemporary Professional Setting." *Accounting, Organizations and Society* 36(3): 135–55.

Bryant, Chris. 2013. "Europe's Spying Businesses Thrive amid Surveillance Uproar." *Financial Time*, July 1. Accessed August 8. http://www.ft.com/cms/s/0/d1b47a24-e232-11e2-a7fa-00144feabdc0.html.

Bryant, Ben. 2015. "UK Police Tried to Buy Hacking Team's Spy Tech, Leaked Emails Show." *VICE News*, July 10. Accessed August 8, 2016. https://news.vice.com/article/uk-police-tried-to-buy-hacking-teams-spy-tech-leaked-emails-show.

Caponetti, Lia. 2016. "Mass Surveillance Technology: Trading Trojan Horses." *Strategic Trade Review* 2(2): 53–71.

Carvalho, Anabela and Jacquelin Burgess. 2005. "Cultural Circuits of Climate Change in U.K. Broadsheet Newspapers, 1985-2003." *Risk Analysis* 25(6): 1457–69.

Coalition Against Unlawful Surveillance Exports (CAUSE). 2014. *A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation.* Accessed July 15, 2016. https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf

Currier, Cora Currier and Morgan Marquis-Boire. 2015. "A Detailed Look at Hacking Team's Emails About Its Repressive Clients." *The Intercept*, July7. Accessed August 8, 2016. https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

Curtin, John Peter and T. Kenn Gaither. 2005. "Privileging Identity, Difference and Power: The Circuit of Culture as a Basis for Public Relations Theory." *Journal of Public Relations Research* 17(2): 91–115.

D'Acci, Julie. 2004. *Television After TV: Essays on a Medium in Translation*. Duke University Press.

Davis, Jeremy Seth. 2016. "Turkey Publishes WhatsApp Messages of Coup Officers." *SC Magazine UK*, July 25. Accessed August 8, 2016. http://www.scmagazineuk.com/news/turkey-publishes-whatsapp-messages-of-coup-officers/article/511482/.

Deibert, Ronald. 2003. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium - Journal of International Studies* 32(3): 501–30.

Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* Information. Cambridge: MIT Press.

Derrida, Jacques. 1976. *Of Grammatology*. Baltimore: Johns Hopkins University Press.

Deutsche Welle. 2013. "Germany Admits Europe's Spy Agencies Cooperate on Surveillance." November 2. Accessed August 8, 2016. http://www.dw.com/en/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903.

Di Salvo, Philip. 2013. "EU Moves toward a Digital Freedom Strategy - European Journalism Observatory" *EJO*, January 7. Accessed June 17, 2016. http://en.ejo.ch/media-politics/eu-digital-freedom-strategy.

Dinev, Tamara, Bellotto Masssimo, Paul Hart, Colautti Christian, Russo Vincenzo, and Serra Ilaria. 2005. "Internet Users, Privacy Concerns and Attitudes towards Government Surveillance-An Exploratory Study of Cross-Cultural Differences between Italy and the United States." *BLED Proceedings*, 30.

Dozier, R. E. and Martha Lauzen. 2000. "Liberating the intellectual domain from the practice: Public Relations, activism and the role of the scholar." *Journal of Public Relations Research* 12(1): 3–22.

Du Gay, Paul, Stuart Hall, Linda Janes, Anders Koed Madsen, Hugh Mackay and Keith Negus. 1997. *Doing Cultural Studies: The Story of the Sony Walkman*. London: Sage.

Dyer-Witherford, Nick. 1999. *Cyber-Marx: Cycles and Circuits of Struggle in High-technology Capitalism*. Urbana: University of Illinois Press.

ECDHR. "The EU's Reaction to Human Rights Violations in Saudi Arabia." Accessed August 8, 2016. http://www.ecdhr.org/the-eus-reaction-to-human-rights-violations-in-saudi-arabia/.

Electronic Frontier Foundation. 2016. "Mass Surveillance Technologies." Accessed August 4, 2016. https://www.eff.org/issues/mass-surveillance-technologies.

European Commission. 2016. "The Importance of the Digital Economy - Growth." Accessed August 7, 2016. https://ec.europa.eu/growth/sectors/digital-economy/importance_en.

European Parliament. 2012. "REPORT on a Digital Freedom Strategy in EU Foreign Policy - A7-0374/2012." *europarl,* November 15. Accessed August 8, 2016. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0374&language=EN.

Falkvinge, Rick. 2015. "European Parliament Gets Everything Right in New Report: Condemns Mass Surveillance, Shames Complicity With NSA, And Demands Encryption,

Net Neutrality, Free/Open Software." *Privacy Online News*, September 11. Accessed June 15, 2016. https://www.privateinternetaccess.com/blog/2015/09/european-parliament-gets-everything-right-in-new-report-condemns/.

Foucault, Michel. 1972. *The Archaeology of Knowledge*. New York: Pantheon.

———. 1977. *Discipline and Punishment*. London: Allen Lane.

———. 1980. *Power/Knowledge*. New York: Pantheon.

Freedom House. 2014. "Freedom of the Net." Accessed July 15, 2016. https://freedomhouse.org/report/freedom-net/freedom-net-2014#.V63YT2Ui2fQ

Fuchs, Christian. 2011. "New Media, Web 2.0 and Surveillance: Web 2.0 Surveillance." *Sociology Compass* 5(2): 134–47.

Golovanov, Sergey. 2013. "Spyware. HackingTeam." *Securelist*, April 23. Accessed July 29, 2015. https://securelist.com/analysis/publications/37064/spyware-hackingteam/.

Gordon, Diana. 1987. "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System." *Politics and Society,* 15: 483-511.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. London: Penguin Books.

Gutwirth, Serge, Ronald Leenes, Paul De Hert, and Yves Poullet. 2012. *European Data Protection: In Good Health?* Dordrecht: Springer Netherlands.

Hacking Team. 2013. "Hacking Team." *The Enemies of Internet*, March 8. Accessed June 15, 2016. http://surveillance.rsf.org/en/hacking-team/.

Hall, Stuart. 1973. *Encoding and Decoding in the Television Discourse.* Centre for Cultural Studies: University of Birmingham.

Hall, Stuart. 1997. *Representation: Cultural Representation and Signifying Practices*. London and Thousand Oaks: Sage.

Harris, Mike. 2014. "EU Lacks a Coherent Strategy on Free Expression in Digital Sphere." *Index on Censorship*, January 10. Accessed August 1, 2016. https://www.indexoncensorship.org/2014/01/eu-lacks-coherent-strategy-free-expression-digital-sphere/.

Hartley, John. 2003. *A short History of Cultural Studies.* London: Sage.

Hayes, Ben. 2016. "Mass Surveillance in the European Union: Communications and Financial Transactions." *Pen America.* Accessed August 8, 2016. https://pen.org/mass-surveillance-european-union-communications-and-financial-transactions-2.

Index on Censorship. 2013. "European Union Urged to Take Lead on Digital Freedom." *IFEX,* June 25. Accessed August 4, 2016. http://www.ifex.org/europe_central_asia/2013/06/25/eu_digital_freedom/.

———. 2013. "Index Policy Paper: Is the EU Heading in the Right Direction on Digital Freedom?" June 20. Accessed July 15, 2016. https://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/.

Jeffries, Adrianne. 2013. "Meet Hacking Team, the Company That Helps the Police Hack You." *The Verge*, September 13. Accessed June 15, 2016. http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers.

Johnson, Richard. 1986. "The Story So Far: And Further Transformations?" In *Introduction to Contemporary Cultural Studies*, edited by David Punter. London: Longman

Krueger, Brian. 2005. "Government Surveillance and Political Participation on the Internet." *Social Science Computer Review* 23(4): 439-452.

Leve, Anabelle M. 2012. "The Circuit of Culture as a Generative Tool of Contemporary Analysis: Examining the Construction of an Education Commodity." *International Conference* 1-12.

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minneapolis Press.

MacAskill, Ewen. 2014. "Edward Snowden's NSA Leaks 'an Important Service', Says Al Gore." *The Guardian,* June 10. Accessed August 4, 2016. https://www.theguardian.com/world/2014/jun/10/edward-snowden-nsa-leaks-important-service-al-gore.

Marquis-Boire, Morgan, John Scott-Railton, Claudio guarnieri and Katie Kleemola. 2014. "Hacking Team's Tradecraft and Android Implant." *The Citizen Lab*, June 24. Accessed July 15, 2016. https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/.

Marx, Gary T. 1988. *Undercover: Police Surveillance in America.* Berkeley: University of California Press.

McRobbie, Angela. 1978. *Working Class Girls and the Culture of Femininity*. London: Hutchinson.

MENASOURCE. 2015. "Top News: EU Report Criticizes Turkey on Human Rights, Freedoms Violations." *Atlantic Council*, November 10. Accessed August 8, 2016. http://www.atlanticcouncil.org/blogs/menasource/top-news-eu-report-criticizes-turkey-on-human-rights-freedoms-violations

Motion, Judy and Shirley Leitch. 2002. "The Technologies of Corporate Identity." *International Studies of Management & Organization* 32(3): 45–64.

Nakhoul, Samia and Nick Tattersal. 2014. "Turkish PM Says Tapes of Talk with Son a Fabrication." *Reuters,* February 25. Accessed June 15, 2016. http://www.reuters.com/article/us-turkey-erdogan-idUSBREA1N1ZX20140225.

Pellot, Brian. 2013. "Index Policy Paper: Is the EU Heading in the Right Direction on Digital Freedom?" *Index on Censorship*, June 20. Accessed July 15, 2016. https://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/.

PEN International. 2014. *Surveillance Secrecy and Self-Censorship: New Digital-Freedom Challenges in Turkey*. Accessed July 20, 2016.

Podesta, Don. 2015. "Watchdogs Under Watch: Media in the Age of Cyber Surveillance." Center for International Media Assistance.

Poster, Mark. 1990. *The Mode of Information.* Cambridge, UK: Polity Press.

———. 1997. *The Second Media Age.* Cambridge, Massachusetts: Polity Press.

Privacy International. 2016. *The President's Men? Inside the Technical Research Department.* Accessed July 15, 2016. https://privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf

Rodriguez, Katitza. 2013. "Internet Surveillance and Free Speech: The United Nations Makes the Connection." *Electronic Frontier Foundation*, June 4. Accessed June 15, 2016. https://www.eff.org/deeplinks/2013/06/internet-and-surveillance-UN-makes-the-connection.

S&D Group. 2015. "Towards a Digital Union." *Socialists and Democrats.* Accessed July 15, 2016.

http://www.socialistsanddemocrats.eu/digitalunion.

Sarabia-Panol, Zeny, and Marianne D. Sison. 2013. "International Public Relations and the Circuit of Culture: An Analysis of Gawad Kalinga." *Asia Pacific Public Relations Journal* 14(1&2): 51–68.

Schaake, Marietje. 2012. "European Parliament Endorses First Ever Digital Freedom Strategy." *Marietje Schaake,* December 10. Accessed August 4, 2016. https://marietjeschaake.eu/european-parliament-endorses-first-ever-digital-freedom-strategy.

———. 2013. "Media: Europe's Spy Technology Expertise Throws up Awkward Questions - Financial Times." *Marietje Schaake*, July 1. Accessed August 11, 2016. https://marietjeschaake.eu/media-europes-spy-technology-expertise-throws-up-awkward-questions-financial-times.

———. 2015. "Report on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries.'" *Marietje Schaake*, September 7. Accessed July 15, 2016. https://marietjeschaake.eu/report-on-human-rights-and-technology-the-impact-of-intrusion-and-surveillance-systems-on-human-rights-in-third-countries.

Scott, Blake, Longo Bernadette, and Katherine V. Wills. 2006. *Critical Power Tools*. Albany: SUNY Press.

Shaw, Craig, and Zeynep Sentek. 2016. "'Citizens Will Be Stripped Naked' by Turkey's Data Law." *ComputerWeekly*, April 5. Accessed August 11, 2016. http://www.computerweekly.com/news/450280254/Citizens-will-be-stripped-naked-by-Turkeys-data-law.

Silver, Vernon. 2011. "Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms." *Bloomberg Business*, December 22. Accessed June 15, 2016. http://www.bloomberg.com/news/articles/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms

Slack, Jennifer Daryl. 1989. "Contextualizing Technology." In *Rethinking Communication: Volume 2-Paradigm Exemplars*, edited by Brenda, Dervin, Lawrence Grossberg, Barbara O'Keefe and Ellen Wartella, 329-345. Newbury Park, CA: Sage.

Sözeri, Efe Kerem. 2015. "Hacked Documents Show Police Used Hacking Software to Track Citizens." 2015. *The Daily Dot*, July 7. Accessed July 15, 2016. http://www.dailydot.com/layer8/hacking-team-turkey/.

Taylor, Bryan C., Christof Demont-Heinrich, Kirsten J. Broadfoot, Jefferson Dodge, and Cuowei Jian. 2002. "New Media and the Circuit of Cyber-Culture: Conceptualizing Napster." *Journal of Broadcasting & Electronic Media* 46(4): 607–29.

The Citizen Lab. 2014. "Mapping Hacking Team's 'Untraceable' Spyware." *The Citizen Lab*, February 17. Accessed July 15, 2016. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

———. 2014. "Morgan Marquis-Boire Writes Piece on Hacking Team Manuals." *The Citizen Lab*, October 31. Accessed July 15, 2016. https://citizenlab.org/2014/10/morgan-marquis-boire-co-authors-article-on-hacking-team/.

———. 2015. "Hacking Team Reloaded." *The Citizen Lab*, March 9. Accessed July 15, 2016. https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

———. 2015. "Open Letter to Hacking Team." *The Citizen Lab*, March 9. Accessed July 15, 2016. https://citizenlab.org/2015/03/open-letter-hacking-team-march-2015/.

———. 2015. "Hacking Team Leak Highlights Citizen Lab Research." *The Citizen Lab*, August 6. Accessed July 15, 2016. https://citizenlab.org/2015/08/hacking-team-leak-highlights-citizen-lab-research/.

———. 2015. "What We Know about the South Korea NIS's Use of Hacking Team's RCS." *The Citizen Lab*, August 9. Accessed July 15, 2016. https://citizenlab.org/2015/08/what-we-know-about-the-south-korea-niss-use-of-hacking-teams-rcs/.

———. 2015. "Research on Hacking Team and FinFisher in the Media." *The Citizen Lab*, November 17. Accessed July 15, 2015. https://citizenlab.org/2015/11/research-on-hacking-team-and-finfisher-highlighted-in-motherboard/.

Thompson, Kenneth. 1997. *Media and Cultural Regulation*. London: Sage.

Thompson, Paul. 2003. "Fantasy Island: A Labour Process Critique of the 'age of Surveillance.'" *Surveillance & Society* 1(2): 138–51.

Verri, Gabriela Jahn, Luiza Bender, and Eduardo Dondonis. 2014. "Government and Corporate Internet." *UFRCS Model United Nations* (2): 411-443.

Wagner, Ben, and Joanna Bronowicka. 2015. "Between International Relations and Arms Controls: Understanding Export Controls for Surveillance Technologies." *Political Science Revolution* 3: 153–65.

Zetter, Kim. 2013. "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments." *WIRED*, June 4. Accessed July 15, 2016. https://www.wired.com/2013/06/spy-tool-sold-to-governments/.

PLAGIARISM STATEMENT

Faculty of Humanities
Version September 2014

PLAGIARISM RULES AWARENESS STATEMENT

Fraud and Plagiarism
Scientific integrity is the foundation of academic life. Utrecht University considers any form of scientific deception to be an extremely serious infraction. Utrecht University therefore expects every student to be aware of, and to abide by, the norms and values regarding scientific integrity.

The most important forms of deception that affect this integrity are fraud and plagiarism. Plagiarism is the copying of another person's work without proper acknowledgement, and it is a form of fraud. The following is a detailed explanation of what is considered to be fraud and plagiarism, with a few concrete examples. Please note that this is not a comprehensive list!

If fraud or plagiarism is detected, the study programme's Examination Committee may decide to impose sanctions. The most serious sanction that the committee can impose is to submit a request to the Executive Board of the University to expel the student from the study programme.

Plagiarism
Plagiarism is the copying of another person's documents, ideas or lines of thought and presenting it as one's own work. You must always accurately indicate from whom you obtained ideas and insights, and you must constantly be aware of the difference between citing, paraphrasing and plagiarising. Students and staff must be very careful in citing sources; this concerns not only printed sources, but also information obtained from the Internet.

The following issues will always be considered to be plagiarism:

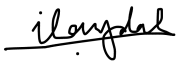
- cutting and pasting text from digital sources, such as an encyclopaedia or digital periodicals, without quotation marks and footnotes;
- cutting and pasting text from the Internet without quotation marks and footnotes;
- copying printed materials, such as books, magazines or encyclopaedias, without quotation marks or footnotes;
- including a translation of one of the sources named above without quotation marks or footnotes;
- paraphrasing (parts of) the texts listed above without proper references: paraphrasing must be marked as such, by expressly mentioning the original author in the text or in a footnote, so that you do not give the impression that it is your own idea;
- copying sound, video or test materials from others without references, and presenting it as one's own work;
- submitting work done previously by the student without reference to the original paper, and presenting it as original work done in the context of the course, without the express permission of the course lecturer;
- copying the work of another student and presenting it as one's own work. If this is done with the consent of the other student, then he or she is also complicit in the plagiarism;
- when one of the authors of a group paper commits plagiarism, then the other co-authors are also complicit in plagiarism if they could or should have known that the person was committing plagiarism;
- submitting papers acquired from a commercial institution, such as an Internet site with summaries or papers, that were written by another person, whether or not that other person received payment for the work.

The rules for plagiarism also apply to rough drafts of papers or (parts of) theses sent to a lecturer for feedback, to the extent that submitting rough drafts for feedback is mentioned in the course handbook or the thesis regulations.
The Education and Examination Regulations (Article 5.15) describe the formal procedure in case of suspicion of fraud and/or plagiarism, and the sanctions that can be imposed.

Ignorance of these rules is not an excuse. Each individual is responsible for their own behaviour. Utrecht University assumes that each student or staff member knows what fraud and plagiarism

Universiteit Utrecht

entail. For its part, Utrecht University works to ensure that students are informed of the principles of scientific practice, which are taught as early as possible in the curriculum, and that students are informed of the institution's criteria for fraud and plagiarism, so that every student knows which norms they must abide by.

I hereby declare that I have read and understood the above.
Name: Ilayda Sarlak Student number: 5682347
Date and signature: 10-10-2016   

Submit this form to your supervisor when you begin writing your Bachelor's final paper or your Master's thesis.

Failure to submit or sign this form does not mean that no sanctions can be imposed if it appears that plagiarism has been committed in the paper.